**The Ethical Impacts of Hacking with a Focus on Gray-Hat Hacking.**

N.L. Hynek, A.A. Thompson, E.T. Newman

Computer Science Department, School of Engineering, Tennessee Technological University, Cookeville, USA

***Abstract*­- The ethics behind hacking has been in debate for as long as it has been in practice. Terms have been given to describe the ethical impact of hacking: White-Hat, Black-Hat and Gray-Hat hacking. We have found the practices and impacts of the aforementioned hacking and it will be discussed later. We have determined that ethical hacking should be taught and that the teaching of this form of hacking is ethical. Finally, we will discuss in whole whether Gray-Hat hacking is ethical or not.**

I. INTRODUCTION

From keylogging to denials-of-service, hacking has been prevalent in today’s robust age of information computing. Hackers have at their leisure a multitude of victims with various tools that allow them to break through cyber walls and steal information. This style of hacking is called Black-Hat hacking. To combat this, many companies have employed ‘hackers’ of their own to reinforce security, White-Hat hackers. This creates a divide between them, and that divide is the use of ethics. However, there is an in-between, a type of hacker that uses both styles of attack for ethically ‘gray’ areas. This type of hacker is called a Gray-Hat hacker. In this essay, we will first introduce the research we’ve done on this topic and present the facts that we have accrued from various sources on databases from the internet. The first part will be about the terminology and defining the various types of hacker. Then, we will discuss the ethical impacts these hackers have on the world around them. Next, we will discuss whether this hacking should or should not be taught in schools, giving information for both sides of the argument. Lastly, we will discuss the ethical ramifications of Gray-Hat hacking and introduce scenarios in which are either ethical or unethical based upon two ethical viewpoints: Virtue ethics and Act Utilitarian ethics.

II. METHODOLOGY

The methods we took to writing this paper are standard and traditional. We scoured many databases for research articles, books, and journals to compile enough information to write a sound paper. All of our sources came from acclaimed databases such as Tennessee Tech’s online library database that spans over 2 million unique articles as well as: IEEE Xplore’s digital library and database, ACM’s digital library and ProQuest’s Computer Science digital library.

III. RESULTS

What is White-Hat hacking? In essence, it is an ethical form of hacking, as opposed to Black-Hat hacking. White-Hat hackers include cyber security analysts and researchers who attempt to break through a systems defense for the purpose of enforcing it. This includes bug detection software. A White-Hat hackers’ job is to find the weakness in software and exploit it to later fix it. This is radically different than Black-Hat hackers who exploit weaknesses for monetary gain in the form of theft. A good example is from *What is Ethical Hacking? White Hat Hackers Explained*[1]. In it, it describes Charlie Miller, a prolific computer whizz and ethical hacker. He used his expertise to uncover major bugs in Apple’s MacBook Air that could have caused some serious issues for the computing firm. He would later find show weaknesses also in Apple’s Safari. These discoveries would earn him $15,000 total.

So, let’s compare this to Black-Hat hacking. Black-Hat hackers have one goal, to exploit weaknesses for selfish gain. In essence, it is remarkably similar to White-Hat hacking, in that exploitations are used for monetary gain. However, the difference is in how Black-Hat hackers are hack for self-serving reasons such as financial gain, revenge or simply, to wreak havoc. The main way Black-Hat hackers gain their money is through theft, fraud, and extortion[1]. This is a polar opposite to the White-Hat hacker’s methods and ideals for monetary accumulation. Black-Hat hacking is also illegal.

Finally, we have Gray-Hat hackers. This type of hacker falls in between Black and White-Hat hackers. Gray-Hats are as quick to protect a company as they are to hack in and commit theft from that same company. Gray-Hats often conduct slightly more morally questionable operations such as hacking groups that they are ideologically opposed to or launching hacktivist protests[1]. These kinds of hackers are primarily driven by curiosity, desire to make the world private and, of course, money. Only Gray-Hat and White-Hat hackers are considered to be ‘ethical’ hackers, as state in *What is Ethical Hacking? White Hat Hackers Explained*[1].

Now that we have discussed what these hackers are, lets discuss how they affect the world around them. In the beginning, most computer network crackers hacked a system simply because it was there. In today’s world, that is no longer the case. In the past several years, Black-Hat hackers have changed from script kiddies who deface web sites to spread worms to earn glory, to real sociopaths intent on doing more devious things, as stated by Dragos Ruiu in *White hat, Gray hat, Black hat* [2]. In fact, hackers secure their computers better than the rest of the computing community and Government agencies and industry could learn from their hacking and protection techniques to improve technology security. The government can learn from two groups as well, the White-Hats and Gray-Hats, who he says research vulnerabilities to protect employers’ and customers’ and who alert user to vulnerabilities. In fact, the government is already using hacker methods such as penetration testing , a search for security holes in a computer system, says Steven Manzuik [2]. This has also led to a multitude of good practices such as the issuing of information security regulations based in part on consultations with hackers, said Mark Loveless, a senior security analyst and BindView and a hacker of 25 years.

This proves that hackers’ importance as teachers is increasing. As software insecurity remains the norm, the number of targets increases and the stakes involved in losing control of financial and confidential data rises, experts say [2]. "Everything you forget, they will find," Roesch said. "It's like the proverbial millions of monkeys typing on typewriters. They have infinite resources and infinite time to find weaknesses in your system." Hackers’ impact on the world of computing is profound, and in some cases, not all that bad.

IV. DISCUSSION

Now that we have talked about what hacking and how it plays a part in the world around us, we now switch our focus to the ethical impacts of said with scenarios and use Act Utilitarianism and Virtue Ethics to analyze these types of hacking. To begin this analysis, let us look at White-Hat hacking. As previously discussed, White-Hat hacking is the only widely accepted form of ‘ethical’ hacking. In *Examples of Ethical Hacking – How Hacking Can Improve Our Lives,*[3] Matt Beauchamp states that,” When used as a means to improve an individual or a company's online defenses, we find this ‘malicious act’ rather beneficial. The practice of breaking into or bypassing an online system or network in order to expose its flaws for further improvement is entirely ethical.” This proves exactly what White-Hat hackers are. In his scenario of breaking into or bypassing an online system or network to expose its flaws for improvement, we will look at it through the lens of Act Utilitarianism. There are two parties in this scenario, the hacker and the employer. The hacker bypasses security and gains money, while the employer fixes flaws in their system and improves network security. Therefore, this, by Act Utilitarianism, is ethical. Now Virtue Ethics- a right action being one that a virtuous person, acting in character, would do in the same circumstances- would also state that this is ethical. The hacker is not gaining anything illegally and is acting in terms of the employer. By these two standards, White-Hat hacking is ethical.

Another example we will use will also be from *Examples of Ethical Hacking – How Hacking Can Improve Our Lives.*[3] “There are a lot of examples of ethical hacking, including one which happened in the early days of computers. Back then, the United States Air Force used it to conduct a security evaluation of an operating system. In doing so, they were able to discover flaws like vulnerable hardware, software, and procedural security.” In Act Utilitarianism, again there are two sides: The hacker or employee, and the Air Force. The hacker gains information and money in exchange for their work while the Air Force gets better network security. This is, therefore, ethical by Act Utilitarianism. By Virtue Ethics, again, it is ethical. The employee is offering their services in exchange for money and rank. They are not exploiting the system for malicious reasons and are keeping the highest form ethical responsibility.

Now to further prove how White-Hat hacking is ethical, and, later, to show the ethical ramification of Gray-Hat hacking, we will look at Black-Hat hacking. As previously stated, Black-Hat hacking is the very definition of unethical hacking. For this example, we will be looking at *A Study on the Morris Worm.*[4] The ethical impact of the Morris Worm was profound, and it changed the general populace’s outlook on internet security. Given a typical situation of the Morris Room such as: a computer gets infected with the Morris Worm and guessed passwords while also causing denial-of-services (DoS). For Act Utilitarianism, the two sides are the hacker and the one being hacked. For the hacker, they didn’t gain anything really, and the one being hacked lost services while also having to replace hardware. This results in a negative, making this unethical by Act Utilitarianism. By Virtue, Ethics, it is also unethical. This worm would infect computers without the user’s permissions and cause DoSs. This is not a virtuous move.

Another example of the same worm[4] is that while it did not gain anything for the hacker and didn’t always cause problems for the user, it provided a huge research opportunity on the worm to shape what network security is today. So, by Act Utilitarianism, there are multiple sides again. One is hacker, who received three years in prison and a $10,000 fine. Another is the person who was hacked, which only had a 1/10 chance of a DoS occurring. The last being the profound research that was given. Given the actual impact of the worm on the users versus the research, we would argue this is ethical for Act Utilitarianism. However, by Virtue Ethics, it is still unethical for the same previously given reason. Overall, the Morris Worm is unethical, and Black-Hat hacking as a whole is unethical.

Now that we have analyzed White and Black-Hat hacking under multiple circumstances, we have to analyze Gray-Hat hacking under the same microscope. In the article *A Mysterious Russian Grey Hat Vigilante has patched over 100,000 routers,*[5] “A Russian-speaking gray-hat hacker has been breaking into people’s MikroTik routers and patching them so they won’t be exploited by crypto-miners and other kind of digital ne’er-do-wells.” Using Act Utilitarianism, we find that the hacker gains the knowledge that they helped someone, while the person who was hacked gained extra security. This leads to a net positive, thus, making this ethical by Act Utilitarianism. However, under Virtue Ethics we find that this is not virtuous, as it is breaking into other people’s security networks and changing things without their permission, which is illegal. Therefore, by Virtue Ethics, this is not ethical.

Further in the article, we find more and more scenarios of the same kind. From 2014 to 2018. “2015 – A group of gray hats, ironically called the White team, releases a piece of malware that closes security holes in several models of Linux routers.” [5]. This scenario falls under the same ethical analysis as previous, ethical by Act Utilitarianism and unethical by Virtue Ethics.

Given this information, this begs the question: Is this really unethical or not? This form of invasive hacking for the good has the potential to be good, however we deem this unethical for one reason alone: permission. However good a person could be in their reason for hacking another, uninvited hacking is unethical and illegal. So while Gray-Hat hacking is in fact, still Gray, we determine that it leans more toward the unethical side because they could have easily broken in the same way and be malicious, it is just too close to be comfortable.

The last question we aim to answer is: Should hacking be taught in university settings? In this age of information technology, hacking is a bigger and bigger threat and as such, is becoming less obscure and the need for people to be able to fight these Black-Hat hackers rise. The benefits and repercussions are both valid: teaching someone how to hack can either be a boon to companies, or a curse. A student who learns to hack could change their grades in the system all the way up to stealing money from their college. On the flip side, a student who learns to hack could fight off hackers for their job or even while still in undergraduate courses. In *The Ethics of Hacking: Should it be Taught?*[6] we find certain situations for both: “For example, in April 2014, a Western University student was caught after hacking into the Canada Revenue Agency.” For against; and, “For academia, it is also a changing environment when universities can play a role in enhancing the corporate and military abilities to respond quickly to threats.” For benefit.

So, given both circumstances we analyze whether it is ethical to teach hacking or not. For Act Utilitarianism, we have the student and the teacher. The student learns valuable skills to use in the world, while the teacher might gain anxiety in the possibility of teaching a hacker. This is ethical then, by Act Utilitarianism as the overall happiness benefits outweigh the negatives. For Virtue Ethics, it’s a little trickier. We have discussed earlier that White-Hat hacking is virtuous while Gray and Black-Hat are not. We think the question lies in how the course is taught as to whether it is virtuous or not. If the course is taught in terms of it being penetration testing for corporation use, as in the employee and employer model, then it is virtuous and therefore ethical. However, if it is taught in terms of personal hacking, it would lean more towards invasive methods and not be virtuous. Overall, we think that most curriculum would lean toward the former therefore making the teaching of hacking in a university standpoint, ethical.

V. CONCLUSION

Together, this concludes our research on hacking. We have discovered and determined what White, Black and Gray-Hat hacking are and their ethical implications, as well as answered the question ‘Is this ethical?’. White-Hat hacking is ethical, while Gray and Black-Hat are unethical. We have also determined that teaching hacking is ethical in most if not all situations.

VI. REFERENCES

[1] C. Hopping, B. Hellard and I. T. Pro, "What is ethical hacking? White hat hackers explained," *IT Pro*, https://search-proquest-com.ezproxy.tntech.edu/compscijour/docview/2137636132/4B80CD8F666B4E11PQ/7?accountid=28833, Nov 2018.

[2] M. Arnone, “White hat, grey hat, black hat”, FCW, <https://fcw.com/articles/2005/10/03/white-hat-gray-hat-black-hat.aspx> (accessed April 30, 2018).

[3] M. Beauchamp, “Examples of Ethical Hacking - How Hacking Can Improve Our Lives”, Ezine Articles, <https://ezinearticles.com/?Examples-of-Ethical-Hacking---How-Hacking-Can-Improve-Our-Lives&id=5428490> (accessed April 30, 2020).

[4] A. Jajoo, “A study on the Morris Worm”, Purdue, https://www.researchgate.net/publication/337499010\_A\_study\_on\_the\_Morris\_Worm, May 2018.

[5] P. Nohe, “A Mysterious Russian Grey Hat Vigilante has patched over 100,000 routers”, The SSL Store, <https://www.thesslstore.com/blog/mysterious-russian-grey-hat-vigilante-patched-over-100000-routers/> (accessed April 30, 2018).

[6] N. Radziwill, J. Romano, D. Shorter, M. C. Benton, “The Ethics of Hacking: Should It Be Taught?”, *Software Quality Professionals*, vol. 18, pp. 11-15, Dec. 2015.